P&R CIO NEWSLETTER
SERVING THE P&R COMMUNITY
MAY 2014

Cybersecurity: A Critical Enabler of Personal and National Security

POINTS OF INTEREST:

- National Initiative for Cybersecurity Education
- National Cybersecurity Workforce Framework
- DoDI 8510.01

In our daily life, we all depend on a safe and resilient cyberspace that allows us to work, communicate, travel, securely purchase goods and services, and much more. Therefore, as the number of cybersecurity attacks multiply, so do widespread concerns about protection, response, laws, regulations, and policies. General Keith Alexander, Director of the National Security Agency, has emphasized the diverse and devastating impacts cyber attacks can have beyond cost, including destroying system data, shutting down power, and even threatening lives.

The Target breach is one recent, high-profile example of a cyber attack that has been costly and potentially catastrophic. So far, Target has spent $61 million on legal fees, software updates, customer reimbursements, and damage control. In 2007, T.J. Maxx and Marshall's parent company paid more than $250 million to address a similar high-profile attack.

President Obama believes that cybersecurity is one of today's most important national security and economic challenges—and one we are not currently adequately equipped to counter. In response, a number of federal government-wide and DoD-wide initiatives have been set in motion to address cybersecurity awareness and preparedness. These include the National Institute of Standards and Technology (NIST)-led National Initiative for Cybersecurity Education (NICE) and the Risk Management Framework (RMF) (see article on Page 2 for details).

NICE is a national campaign spanning more than 20 federal departments and agencies that seeks to improve the cyber behavior, skills, and knowledge of every segment of the population, enabling a safer cyberspace. The initiative is comprised of four components:

- **Public Awareness:** uses public service campaigns to promote cybersecurity and responsible internet use, and aims to make cybersecurity a popular educational and career pursuit for students
- **National Education:** enhances formal cybersecurity education programs at all levels, with a focus on science, technology, and other disciplines that help prepare a pipeline of skilled workers
- **Workforce Structure:** evaluates the workforce's professionalization, recommends best practices for anticipating future cybersecurity needs, and defines national strategies for recruitment and retention
- **Workforce Training and Professional Development:** improves training and professional development programs for the existing federal cybersecurity workforce

To further support the development and maintenance of a highly-skilled workforce, NICE also developed the National Cybersecurity Workforce Framework, which promotes consistency by providing federal government-wide definitions for cybersecurity-related roles and terms.

Although there is still much to be done in the cybersecurity arena, federal government-championed initiatives such as NICE will continue to improve our nation's posture to respond to the range of dynamic threats.

Sources:

Jayakumar, Amrita. "Data Breach Hits Target Profits." *The Washington Post.* 27 Feb 2014.

NICE: http://csrc.nist.gov/nice

DoDI 8510.01: http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

DoD Adopts Common Federal Cybersecurity Terminology through Transition to Risk Management Framework

In the spirit of working collaboratively to strengthen our nation's cybersecurity posture across the federal government, representatives from the defense, civil, and intelligence communities, including NIST and the Committee on National Security System (CNSS), have worked together to find common ground related to cybersecurity guidance. On March 12, 2014, the DoD CIO released DoDI 8510.01, which replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) with the RMF.

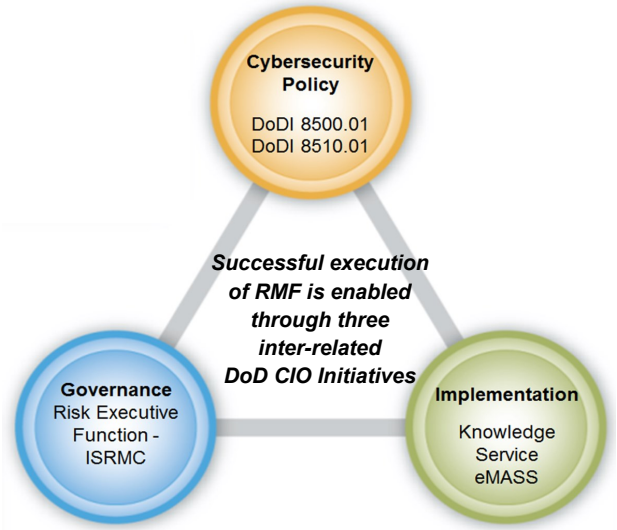
Why the Transition?

The transition to RMF implements common cybersecurity terminology across defense and civilian networks, which streamlines processes and allows for easier interconnection and information sharing. The framework also achieves cost savings by reducing the need to recertify systems shared across organizations.

How is RMF Different from DIACAP?

RMF is similar to DIACAP but includes several small changes that promote consistency and enhance the process:

- Uses different role names (e.g., Information Assurance Officer under DIACAP vs. Information System Security Manager under RMF)
- Directs the use of the Committee on National Security Systems Instruction (CNSSI) 1253 for Security Control Categorization and Selection and use of overlays
- Defines what IT should undergo the full RMF lifecycle
- Promotes developmental test and evaluation (DT&E) and operational test and evaluation (OT&E) integration
- Codifies reciprocity
- Strengthens enterprise-wide IT governance



What are RMF's Benefits?

- Aligns the DoD with the rest of the federal government, promoting interoperability and information sharing
- Incorporates cybersecurity early in the acquisition lifecycle, reducing time and money spent bolting on security late in system development
- Enables deployment of enterprise-wide cybersecurity solutions (i.e., build once, use many) via inheritance of centrally built, hosted, and authorized capabilities
- Incorporates risk management considerations, providing organizations a true picture of a vulnerability caused by non-compliant controls and other risk factors (i.e., likelihood, threat, and impact)
- Enables organizations to accept approvals by other organizations for interconnection or reuse without retesting

What's Ahead for RMF?

Transitioning to RMF marks the adoption of a single set of risk management standards for federal IT systems and new processes within the system development lifecycle. For example, RMF will be used to determine if a system meets baseline security expectations required for initial authorization. Moreover, it will also support a Continuous Monitoring Program to evaluate systems for ongoing authorization, including three-year accreditations. In this way, the framework emphasizes ongoing checks for information security and timely correction of deficiencies.

Want to Learn More?

Visit **DISA's Information Assurance Support Environment Web site:** http://iase.disa.mil/index2.html

Contact the **RMF Technical Advisory Group:** osd.rmftag-secretariat@mail.mil

Acronyms Defined | ATO: Authority to Operate | C&A: Certification and Accreditation
DoDI: DoD Instruction | eMASS: Enterprise Mission Assurance Support Service
IA: Information Assurance | ISRMC: Information Security Risk Management Committee

Content and Images Source: DoD CIO Briefing "DIACAP to RMF Transformation," 26 March 2014